CLAIMS

What is claimed is:

1. A method for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the steps of:

(a) signing a phrase by a security chip of the server using an encryption key;

(b) associating the signed phrase with the remote user;

(c) signing the phrase with an encryption key obtained by the security chip when a request for access to the computer network is received from the remote user;

(d) comparing the phrase signed with the obtained encryption key with the signed phrase associated with the remote user; and

(e) granting access to the remote user if the phrase signed with the obtained encryption key is the same as the stored signed phrase associated with the remote user.

2. The method of claim 1, wherein the signing step (a) comprises:

(a1) creating a public key and a private key pair for the remote user by the security chip; and

(a2) signing the phrase with the private key of the remote user by the security chip.

3. The method of claim 2, wherein the associating step (b) further comprises:

(b1) storing the signed phrase associated with the remote user.

4. The method of claim 3, wherein the signing (c) comprises:

(c1) receiving a password from the remote user;

(c2) sending the received password and the phrase to the security chip;

(c3) loading the private key of the remote user; and

(c4) signing the phrase with the loaded private key by the security chip.

5. The method of claim 4, wherein the comparing step (d) comprises:

(d1) comparing the phrase signed with the loaded private key with the stored signed phrase associated with the remote user.

6. The method of claim 5, wherein the granting step (h) comprises:

(e1) granting access to the remote user if the phrase signed with the loaded private key is the same as the stored signed phrase associated with the remote user.

7. The method of claim 1, wherein the signing step (a) comprises:

(a1) signing a password for the remote user by the security chip with a private key of the security chip.

8. The method of claim 7, wherein the associating step (b) comprises:

(b1) associating the signed password with the remote user; and

(b2) storing the signed password associated with the remote user.

9. The method of claim 8, wherein the signing step (c) comprises:

(c1) receiving the password from the remote user;

(c2) sending the received password to the security chip;

(c3) loading the private key of the security chip; and

(c4) signing the received password with the loaded private key by the security chip.

10. The method of claim 9, wherein the comparing step (d) comprises:

(d1) comparing the signed received password with the stored signed password.

11. The method of claim 10, wherein the granting step (e) comprises:

(e1) granting access to the remote user if the signed received password is the same as the stored signed password.

12. The method of claim 1, wherein the signing step (a) comprises:

(a1) creating a blob for the remote user, wherein the blob comprises a password for the remote user signed with a private key of the security chip.

13. The method of claim 12, wherein the associating step (b) comprises:

(b1) associating the blob with the remote user; and

(b2) storing the blob associated with the remote user.

14. The method of claim 13, wherein the signing step (c) comprises:

(c1) receiving the password from the remote user;

(c2) sending the received password and the blob associated with the remote user to the security chip; and

(c3) decrypting the blob associated with the remote user using a public key of the security chip to obtain the stored password.

15. The method of claim 14, wherein the comparing step (d) comprises:

(d1) comparing the stored password with the received password.

16. The method of claim 15, wherein the granting step (e) comprises:

(e1) granting access to the remote user if the stored password is the same as the received password.

17. The method of claim 1, further comprising:

(f) denying access to the remote user if the phrase signed with the obtained encryption key is the same as the stored signed phrase associated with the remote user.

18. A method for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the steps of:

(a) creating a public key and a private key for the remote user by a security chip of the server;

(b) signing a phrase with the private key of the remote user by the security chip;

(c) associating the signed phrase with the remote user;

(c) storing the signed phrase associated with the remote user;

(d) receiving a password from the remote user;

(e) sending the received password and the phrase to the security chip;

(f) loading the private key of the remote user;

(g) signing the phrase with the loaded private key by the security chip;

(h) comparing the phrase signed with the loaded private key with the stored signed phrase associated with the remote user; and

(g) granting access to the remote user if the phrase signed with the loaded private key is the same as the stored signed phrase associated with the remote user.

19. A method for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the steps of:

(a) signing a password for the remote user by a security chip of the server with a private key of the security chip;

(b) associating the signed password with the remote user;

(c) storing the signed password associated with the remote user;

(d) receiving the password from the remote user;

(e) sending the received password to the security chip;

(f) loading the private key of the security chip;

(g) signing the received password with the loaded private key by the security chip;

(h) comparing the signed received password with the stored signed password; and

(i) granting access to the remote user if the signed received password is the same as the stored signed password.

20. A method for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the steps of:

(a) creating a blob for the remote user, wherein the blob comprises a password for the remote user signed with a private key of a security chip of the server;

(b) associating the blob with the remote user;

(c) storing the blob associated with the remote user;

(d) receiving the password from the remote user;

(e) sending the received password and the blob associated with the remote user to the security chip;

(f) decrypting the blob associated with the remote user using a public key of the security chip to obtain the stored password;

(g) comparing the stored password with the received password; and

(h) granting access to the remote user if the stored password is the same as the received password.

21. A computer readable medium with program instructions for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the instructions for:

(a) signing a phrase by a security chip of the server using an encryption key;

(b) associating the signed phrase with the remote user;

(c) signing the phrase with an encryption key obtained by the security chip when a request for access to the computer network is received from the remote user;

(d) comparing the phrase signed with the obtained encryption key with the signed phrase associated with the remote user; and

(e) granting access to the remote user if the phrase signed with the obtained encryption key is the same as the stored signed phrase associated with the remote user.

22. The medium of claim 21, wherein the signing instruction (a) comprises instructions for:

(a1) creating a public key and a private key pair for the remote user by the security chip; and

(a2) signing the phrase with the private key of the remote user by the security chip.

23. The medium of claim 22, wherein the associating instruction (b) further comprises instructions for:

(b1) storing the signed phrase associated with the remote user.

24. The medium of claim 23, wherein the signing instruction (c) comprises instructions for:

(c1) receiving a password from the remote user;

(c2) sending the received password and the phrase to the security chip;

(c3) loading the private key of the remote user; and

(c4) signing the phrase with the loaded private key by the security chip.

25. The medium of claim 24, wherein the comparing instruction (d) comprises instructions for:

(d1) comparing the phrase signed with the loaded private key with the stored signed phrase associated with the remote user.

26. The medium of claim 25, wherein the granting instruction (h) comprise instructions for:

(e1) granting access to the remote user if the phrase signed with the loaded private key is the same as the stored signed phrase associated with the remote user.

27. The medium of claim 21, wherein the signing instructions (a) comprises instructions for:

(a1) signing a password for the remote user by the security chip with a private key of the security chip.

28. The medium of claim 27, wherein the associating instruction (b) comprises instructions for:

(b1) associating the signed password with the remote user; and

(b2) storing the signed password associated with the remote user.

29. The medium of claim 28, wherein the signing instruction (c) comprises instructions for:

(c1) receiving the password from the remote user;

(c2) sending the received password to the security chip;

(c3) loading the private key of the security chip; and

(c4) signing the received password with the loaded private key by the security chip.

30. The medium of claim 29, wherein the comparing instruction (d) comprises instructions for:

(d1) comparing the signed received password with the stored signed password.

31. The medium of claim 30, wherein the granting instruction (e) comprises instructions for:

(e1) granting access to the remote user if the signed received password is the same as the stored signed password.

32. The medium of claim 31, wherein the signing instruction (a) comprises instructions for:

(a1) creating a blob for the remote user, wherein the blob comprises a password for the remote user signed with a private key of the security chip.

33. The medium of claim 32, wherein the associating instruction (b) comprises instructions for:

(b1) associating the blob with the remote user; and

(b2) storing the blob associated with the remote user.

34. The medium of claim 33, wherein the signing instruction (c) comprises instructions for:

(c1) receiving the password from the remote user;

(c2) sending the received password and the blob associated with the remote user to the security chip; and

(c3) decrypting the blob associated with the remote user using a public key of the

security chip to obtain the stored password.

35. The medium of claim 34, wherein the comparing instruction (d) comprises instructions for:

(d1) comparing the stored password with the received password.

36. The medium of claim 35, wherein the granting instruction (e) comprises instructions for:

(e1) granting access to the remote user if the stored password is the same as the received password.

37. The medium of claim 31, further comprising instructions for:

(f) denying access to the remote user if the phrase signed with the obtained encryption key is the same as the stored signed phrase associated with the remote user.

38. A computer readable medium with program instructions for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the instructions for:

(a) creating a public key and a private key for the remote user by a security chip of the server;

(b) signing a phrase with the private key of the remote user by the security chip;

(c) associating the signed phrase with the remote user;

(c) storing the signed phrase associated with the remote user;

(d) receiving a password from the remote user;

(e) sending the received password and the phrase to the security chip;

(f) loading the private key of the remote user;

(g) signing the phrase with the loaded private key by the security chip;

(h) comparing the phrase signed with the loaded private key with the stored signed phrase associated with the remote user; and

(g) granting access to the remote user if the phrase signed with the loaded private key is the same as the stored signed phrase associated with the remote user.

39. A computer readable medium with program instructions for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the instructions for:

(a) signing a password for the remote user by a security chip of the server with a private key of the security chip;

(b) associating the signed password with the remote user;

(c) storing the signed password associated with the remote user;

(d) receiving the password from the remote user;

(e) sending the received password to the security chip;

(f) loading the private key of the security chip;

(g) signing the received password with the loaded private key by the security chip;

(h) comparing the signed received password with the stored signed password; and

(i) granting access to the remote user if the signed received password is the same as the stored signed password.

40. A computer readable medium with program instructions for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the instructions for:

(a) creating a blob for the remote user, wherein the blob comprises a password for the remote user signed with a private key of a security chip of the server;

(b) associating the blob with the remote user;

(c) storing the blob associated with the remote user;

(d) receiving the password from the remote user;

(e) sending the received password and the blob associated with the remote user to the security chip;

(f) decrypting the blob associated with the remote user using a public key of the security chip to obtain the stored password;

(g) comparing the stored password with the received password; and

(h) granting access to the remote user if the stored password is the same as the received password.

41. A system, comprising:

an encryption key associated with a remote user;

a table, wherein the table stores a signed phrase associated with the remote user, wherein the stored signed phrase is signed with the encryption key associated with the remote user; and

a security chip, wherein when the security chip receives a request for access to the system from the remote user, the security chip signs a phrase with the encryption key associated with the remote user,

wherein the system compares the phrase signed with the encryption key associated with the remote user with the stored signed phrase associated with the remote user, wherein the system grants access to requesting remote user if the phrase signed with the encryption key associated with the remote user is the same as the stored signed phrase associated with the remote user.